(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11623 A1

(51) International Patent Classification[7]: G11B 20/00, G06F 1/00

(21) International Application Number: PCT/GB00/02985

(22) International Filing Date: 3 August 2000 (03.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9918403.8 4 August 1999 (04.08.1999) GB

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL FEDERATION OF THE PHONOGRAPHIC INDUSTRY** [CH/CH]; Utoquai 37, P.O. Box 581, CH-8024 Zurich (CH).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **JESSOP, Paul, Mark,** **Brand** [GB/GB]; County Cottage, 84 Common Road, Kensworth, Dunstable, Beds LU6 3RG (GB).

(74) Agents: **MUSKER, David, Charles** et al.; R.G.C. Jenkins & Co., 26 Caxton Street, London SW1H 0RJ (GB).

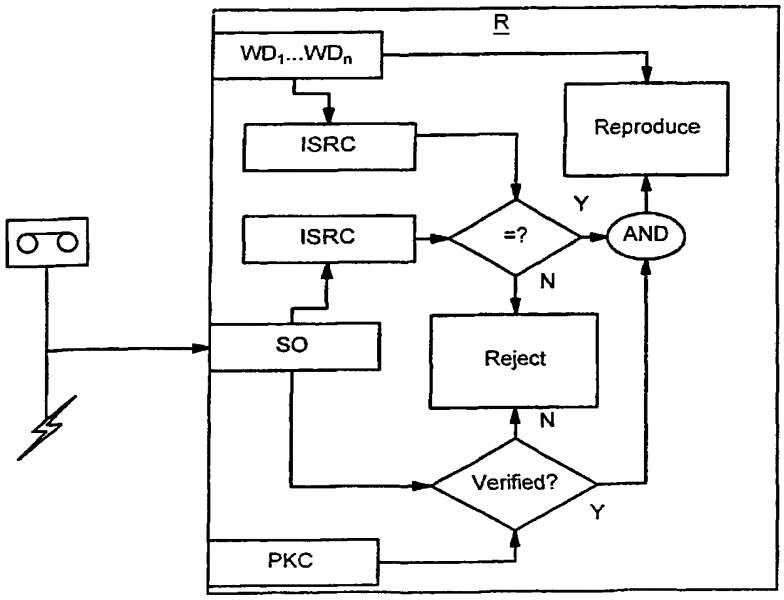
(81) Designated States *(national)*: CA, JP, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: REPRODUCTION CONTROL SYSTEM



(57) Abstract: A method of selectively transferring a digital data file onto a medium for enabling mass reproduction of the digital data file, comprising: obtaining said data file; receiving authorisation data including encrypted data derived from a file identity code substantially uniquely identifying said data file; deriving said file identity code from said data file; comparing said file identity code with said encrypted data and inhibiting transferral of the data file onto the medium if the encrypted data does not correspond to said file identity code.

WO 01/11623 A1

REPRODUCTION CONTROL SYSTEM

Field of the Invention

The present invention relates to system for restricting the copying of digitally represented matter, such as digital audio, video or graphics data or software, or a combination of these, onto a medium adapted for making multiple copies.

Background to the Invention

Large-scale piracy of sound, video or data recordings generally requires the production of a master from which unauthorised copies can be mass-produced. The replication of, for example, compact discs (CD's) and Digital Versatile Discs (DVD's), requires a chain of operations often involving different parties. To produce a CD or DVD, a master tape of a recording is submitted by a music production company to a CD or DVD mastering company which produces metal stampers. The metal stampers are then used by a CD or DVD manufacturing company to 'stamp' or mould the CD's or DVD's, which are then overprinted with a label, packaged and distributed. One of the problems faced by the recording industry is the use of the facilities of mastering and manufacturing companies by pirates, alongside legitimate users, without being detected. The mastering or manufacturing company taking the order does not have the means to check whether an order is authorised by the copyright owner, or may negligently or deliberately carry out an unauthorised order.

Digital audio and video content may also be distributed electronically, for example as MP3 or MPEG files. These files are uploaded onto a website so that customers can purchase and download the desired files. The distribution of files in this way also involves a chain of intermediaries. For example, a master tape may be encoded by a studio into files of the desired digital format, the encoded files are uploaded onto a server connected to the

Internet, and are downloaded, via servers operated by Internet Service Providers (ISP's), onto the user's computer or digital player. The operators of the servers may be liable for copyright infringement if the distribution of the files is not authorised by the copyright owner, but it is difficult for the operators to determine whether the distribution is authorised or not.

The WIPO Copyright Treaty (WCT) and Performances and Phonograms Treaty recognise that the digital dissemination of copyright works may be restricted and monitored by the use of 'technological measures' and 'rights management information' and oblige contracting states to provide adequate and effective legal remedies against the circumvention of such technological measures and the removal or alteration of rights management information. The recent draft EU copyright directive seeks to implement these legal remedies and to provide a definition of 'technological measures'. Hence, a legal framework is being put in place for greater control over the dissemination of digital copyright works by technical means. What is now required is effective technical means of copy protection and rights management.

Under the Source ID (SID) system, CD mastering companies include, on the stampers which they produce, a visible code which is then carried by all CD's made from those stampers, allowing the CD's to be traced back to the mastering company. However, a pirate may obliterate this code from the stampers before sending them to the manufacturing company. Moreover, the mastering company can claim ignorance that the copying was unauthorised. The SID system is a joint venture between the International Federation of the Phonographic Industry (IFPI) and Philips consumer electronics B.V. Eindhoven, the Netherlands and is described in "Implementation of the SID code", IFPI 1995.

There have been various proposals to add watermarks to content including audio, video, image files or data, where the watermark identifies the copyright information of the content. Watermarking allows the copyright

owner of the content to be easily identified, which assists legal action but does not prevent the content from being copied.

Statement of the Invention

According to the present invention, there is provided a copy protection system in which a file is accompanied by a digital signature of information uniquely identifying the file, reproduction of the file being prevented unless the digital signature is verified and matches the identifying information. It will be understood that the term "file" is intended to cover terms such as "data", "content", or "data content".

The identifying information may be embedded as a code within the file, such as a watermark. Alternatively, the identifying information may be derived from characteristics of the file without modifying the file so as to embed a code.

The file may be further accompanied by reproduction command information including one or more of: a code identifying the party authorised to reproduce the file, an expiry time stamp, a designated geographical location and a designated reproduction apparatus. Preferably, the reproduction command information is digitally signed together with the file identifying information.

The present invention extends to methods and apparatus for generating the necessary data for the system, a reproduction method and apparatus in which reproduction is inhibited unless the data are validated, a computer program for carrying out the method, a signal including the necessary data and a medium carrying the necessary data.

Brief Description of the Drawings

Specific embodiments of the present invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 is a diagram of a system by which a verifiable order is generated;

Figure 2 is a diagram of a system by which the verifiable order is verified;

Figure 3 is a diagram of an automated apparatus for submitting a verifiable order;

Figure 4 is a diagram of mastering apparatus for receiving and processing a verifiable order to produce a master, and

Figure 5 is a diagram of an Internet server for receiving a verifiable order and selectively making files available on the Internet if the order is verified.

Description of Embodiments

Order Generation

In the system of Figure 1, a producer P generates a set of data files D_1 to D_n, such as a set of digital audio tracks. For each audio track, the producer generates a corresponding recording identification code, such as an International Standard Recording Code (ISRC), as defined by International Standard ISO 3901. The ISRC uniquely identifies the producer P, the country of residence of the producer P and the year of allocation of the ISRC, and further includes a sequential code used by the producer to identify uniquely each track produced. The skilled reader will appreciate that ISRC's are used specifically to identify audio tracks and that other identifying marks or codes would be used where the copy protection system of the present invention is used to protect other data, such as: software; graphics; images; video clips; and, text and the like.

The producer P is issued with a private encryption key K by a certification authority CA, which also issues the producer's public key in a public key certificate PKC digitally signed with the certification authority's

private key. The public key certificate PKC is freely available, for example from a web site or on request via e-mail from the producer P or the certification authority CA.

The producer P embeds into each of the audio tracks the corresponding ISRC, by means of a watermarking process, to produced watermarked data files WD_1 to WD_n. For example, if the audio data is to be recorded in audio CD format, the ISRC may be spread-spectrum encoded as low level noise added to the CD format data. Numerous techniques have been proposed to include watermarking data in audio. The characteristic features of the watermarking technique are that the reproduction quality of the data file should not be substantially impaired by the addition of the watermark and that the watermark is not readily discernible or removable unless the precise technique used to embed the watermark is known. The individually watermarked data files WD_1 to WD_n are then recorded onto a suitable carrier, such as a digitally recordable disc or tape, or are transferred over a communications channel to the recipient of the order.

The watermark of each track may include, in addition to the respective ISRC, a digital signature of the ISRC created using the producer's private key, confirming that the watermark was added by the producer P. It is not necessary that the ISRC be generated and the watermark be applied at the time of generating the order; these steps may be performed in advance, for example immediately after the original recording of the track is made.

As an alternative to the use of watermarking, a characteristic code is generated from the content of the data file by means of a suitable algorithm selected so that no two different files of a specified type should generate the same characteristic code. For audio data files, TESPAR (Time Encoded Signal Processing and Recognition) fingerprints, as described for example in US 5,519,805, may be used as characteristic codes. For software files, a hash function may be used. This non-watermarking technique is preferred when the data content of the data file cannot be modified without rendering the data

file unusable, such as when the data file contains a computer program. To provide evidence of copyright ownership, the characteristic code of each data file may be transmitted together with a corresponding reference code, such as an ISRC, to an administering authority where the transmitted information is stored in a publicly accessible database. The order may specify a list of the characteristic codes of the data files, or the ISRC's corresponding to the data files.

The producer P also generates order data O, which includes details of the current order, such as the identity of the party to whom the order is to be sent, and/or the date and the time of the order and the duration of validity of the order. As a further option, the producer P may specify a geographical location or range of geographical locations at which the order is to be carried out, or the identity of the equipment on which the order is to be carried out.

The producer P uses its private key to produce a digital signature of the list of ISRC's for the audio data files and of the order data O, to produce a signed order SO. It will be appreciated that the length of the signature may vary between systems implementing the present invention and between successive signatures produced in a given system. The digital signing of the order O prevents pirates from intercepting and altering the details of the order. The signed order SO may be stored on the same digitally recordable medium as the watermarked data files WD, on a separate recordable medium such as a floppy disc or smart card or plain text in paper format or transferred over the communications channel to the recipient of the order. In this way, the ISRC's are bound to the data files, and the ISRC's and the identity of the producer P are bound to the order data O.

An example of a simple form of signed order SO in the form of a text file appears below:

CD Order:

Track 1 *ISRC=GB-98-ABC-01001*

Track 2 *ISRC=GB-98-ABC-01002*

...

Track 12 ISRC=GB-98-ABC-01012

Total Tracks=12

Order Criteria:

...

Begin Signature

K39SNMRIOR2TMSUA3M34JSL

85K45KAMAZXVBCV565D5E5E

End Signature

Order Verification

The process of verification of the order will now be described with reference to Figure 2. A recipient R receives the watermarked data files WD_1 to WD_n and screens them for the presence of watermarks using a reverse algorithm of that used to embed the watermarks. If the watermarks are present, a list of ISRC's for the audio files is derived from the watermarks.

In the alternative system in which watermarking is not used, the recipient R generates characteristic codes of the data files using the same algorithm as was used by the producer P, and interrogates the database of characteristic codes maintained by the administering authority. If the characteristic code of any of the data files matches an entry in the database, the corresponding ISRC code is retrieved from the database. In this way, the ISRC may be bound to a file without the need for watermarking. Suitable security measures, such as digital signatures and/or a secure connection, may be used when interrogating the database. In the alternative in which the characteristic codes are listed in the signed order, the database need not be interrogated.

The recipient R also verifies the signature of the producer P on the signed order SO using the public key extracted from the public key certificate PKC for the producer P. The public key certificate PKC may be sent to the

recipient by the producer P using the same medium as the signed order SO, or may have been obtained in advance from the producer or from a certification authority.

Preferably, the recipient R maintains a database of the identities and public key certificates of known legitimate producers P, the database being updated by downloading information from a trusted web site operated by the administering authority, or by dialling in directly via a secure communications link to a server operated by the administering authority. If the identity or public key certificate PKC of the producer P does not appear on this database, the order is not executed.

If the signature is verified, the ISRC list contained in the signed order is compared with the ISRC's extracted from the watermarks or from the characteristic code database. If the ISRC's match, the recipient processes the order by reproducing the data files in a form enabling mass distribution.

The recipient R also checks the content of the order data O. If the order data O includes a time stamp and validity duration, the time of receipt of the order is compared with the time stamp on the order; if the difference is greater than the validity duration, the order is rejected. To avoid tampering with the local clock so that an out-of-date order can be validated, the computer 2 may be connected to a time reference, such as a network time source running an SNTP (Simple Network Time Protocol) such as SNTPv4 defined in IETF RFC 2030, or preferably an NTP (Network Time Protocol) incorporating security protocols such as NTPv3 defined in IETF RFC 1305. Reference is made to Technical Standard IA-8310: Laboratory Network Time Protocols (NTP/SNTP). Alternatively, the internal clock of the computer 2 may be used. The use of time stamps and validity durations may prevent a pirate from intercepting and replaying an order to another recipient, and subsequently using the result of the duplicate order.

If the order data O includes a code identifying an intended recipient, the recipient R compares this code with its own code and rejects the order if

and an indication of whether the order was accepted or rejected, and optionally the reason for rejection. The acknowledgement message may additionally or alternatively be sent to a third party responsible for monitoring use of the order checking system. If the order was rejected, the third party may then investigate whether the order was fraudulent.

It will be appreciated that the order checking equipment may be configured to output a message to the operator informing him that the execution of an order for which the signed order is not verified, or for which the ISRC's do not match may constitute a copyright infringement. In the event that the rejection is overridden by the operator, the equipment may be configured to record each such "rejection override" in a memory of the equipment, not accessible to the operator or user thereof. Alternatively a record of each "rejection override" may be simultaneously transmitted to a third party responsible for monitoring the use of the order checking system.

Specific Applications

A more specific embodiment of the invention, applied to a laser beam recorder (LBR) for mastering music CD's and to an Internet server, will now be described with reference to Figures 3, 4 and 5. Figure 3 shows apparatus present at the premises of the producer P. A general purpose computer 2, such as a personal computer (PC), is connected to a data file input device 4, such as a CD drive. Audio data tracks previously recorded on recordable CD's are read by the CD drive and are stored as the data files D_1 to D_n on a mass storage device 6, such as a large capacity hard disc. The computer 2 may be connected to a time reference 7, such as a network time source running an SNTP or an NTP as discussed above.

Application software running on the computer 2 creates a set of ISRC's corresponding to the data files D_1 to D_n, which ISRC's are stored in a file with links to the corresponding data files D_1 to D_n. The software then processes each data file D in turn by embedding the corresponding ISRC as a

watermark, and optionally by converting the content to another format if this is required, and stores the resultant watermarked data files WD_1 to WD_n on the mass storage device 6.

The application prompts the user to enter a user definable portion of the order data O. The user definable portion may include the identity of the intended recipient and the validity duration of the order. There may be stored on the computer a database of the identities and locations of the reproduction facilities of possible recipients, such that the application software looks up the geographical location corresponding to the intended recipient indicated by the user, and adds the location information to the order data O.

The application then generates a time stamp which is added to the order data O, using one of the internal clocks of the computer 2, or the time reference 7, such as a network time source running an SNTP or NTP as discussed above.

The completed order data O and the ISRC list are then digitally signed using the producer's private key. The digital signature is derived by generating a hash of the input data, using for example the Secure Hash Algorithm (SHA), and encrypting the hash using the private key and a suitable algorithm, such as RSA encryption.

For reasons of security, the private key may be stored and the signature algorithm performed within a smart card 9 removably inserted in a smart card I/O device 8 connected to the computer 2, so that it is impossible to derive the private key by scanning the memory or storage devices of the computer 2. Additional security measures may be provided, such as PIN's or biometric scanning, to ensure that only authorised users can use the smartcard to issue a signed order.

In this embodiment, the computer 2 is connected to a communications network, such as a PSTN or ISDN, or to a leased line, using an appropriate communications device 10, such as a modem or terminal adapter. The watermarked or registered data files WD and signed order SO are transmitted

over the communications link to the order recipient, two alternative examples of which will now be described.

In the embodiment shown in Figure 4, the recipient of the order is a CD mastering facility MF. A general purpose computer 12 is connected to the communications link by an appropriate communications interface 14, so as to receive the watermarked or registered data files WD and signed order SO from the producer P and to store them in a mass storage device 16, such as a large hard disc. A GPS receiver 17 connected to the computer 12 provides location information. As previously described, the computer 2 may be connected to a time reference (not shown) for time information, such as a network time source running an SNTP or an NTP. Alternatively, the internal clock of the computer may be used for this function.

Preferably, the computer 12 stores the signed order SO in an archive, together with the recorded time of receipt, so as to provide evidence of the order. The signed order SO and time of receipt may be transmitted to a remote server operated by an authority responsible for administering the rights management system.

Application software running on the computer performs the ISRC checking and signature verification of the signed order, as described above with reference to Figure 2. The public key certificate PKC of the producer P may be transmitted from the producer P to the order recipient R with the watermarked data files WD and the signed order SO, or may have been obtained and stored previously by the order recipient. If the ISRC's match, the signature is verified and any other details of the order data O are correct, the computer 12 outputs the data files WD to a laser beam recorder (LBR) 18 which records the files on a master disc. Otherwise, the application software terminates and the files WD are not recorded. Examples of suitable computer controlled LBR's are the OMP DMS 8000, Nimbus Universal Ultra Violet Dual Beam Recorder, Sony WMC-3700 and Panasonic Dual Beam LBR.

Such equipment is usually integrated with signal processing systems from Media Morphics, Kenwood and DCA.

In an alternative embodiment shown in Figure 5, the recipient R operates a server 20 connected to the Internet 26. The server 20 receives the data files WD and the signed order SO on the communications link by means of an appropriate interface device 22, and stores the received files on a holding storage device 25, such as a hard disc. The server 20 performs the signature verification of the signed order SO and checks that the files match the list of ISRC's in the signed order SO, as described above with reference to Figure 2. Any other details of the order data O are also checked, as described above with reference to Figure 2.

If the verification process is successful, the server 20 transfers the watermarked data files to an Internet-accessible storage device 24, such as an array of hard discs. The server 20 allows downloading of files stored in the Internet-accessible storage device 24 by means of HTTP, FTP or other protocols. However, if the order is not verified, the files are not transferred to the Internet-accessible storage device. Instead, a report may be transmitted to an administering authority, including for example the signed order SO and a record of when and from where it was received. The report may be transmitted automatically via a suitable communications medium, such as the Internet 26.

For greater security, the server 20 may be arranged as a recipient server for receiving files and signed orders from producers, connected via a network or cable connection to a separate Internet server. The recipient server is configured as a firewall to prevent access to received files from the Internet before they are transferred to the Internet server.

Mass reproduction equipment incorporating an embodiment of the present invention should hinder use by pirates. For example, if an order is created by a pirate from tracks copied from commercially available CD's, the pirate may not be able to derive the ISRC's of the tracks from the watermarks

and therefore cannot create an order matching the watermarked ISRC's. Even if the pirate can derive the ISRC's from the watermarks, the pirate cannot forge a signature of a *bona fide* producer on the signed order SO, since the key required to generate the signature is difficult to obtain. If the pirate obtains a legitimate key pair, for example by establishing a front as a legitimate producer, then the involvement of the legitimate producer in producing unauthorised copies of tracks is evident from the signed order SO, and the key pair may then be revoked.

Although the system may be circumvented by order recipients who do not adopt the system, it will be in the interests of legitimate order recipients to adopt the system so as to avoid inadvertently assisting in piracy.

In the embodiments described above with reference to Figures 4 and 5, a computer is used automatically to control whether or not reproduction is carried out. The computer may be a general purpose computer connected to the reproduction apparatus, or may be integrated with the reproduction apparatus in such a way that the data files cannot be reproduced by bypassing the order verification process. As an alternative, the general purpose computer may indicate to an operator whether or not an order is validated without automatically inhibiting reproduction, and the operator may then decide whether to proceed with the order. A subsequent inspection of the archived orders of a recipient and comparison with evidence of orders actually processed by the recipient will then establish whether a recipient failed to use the validation process for some of the orders, or deliberately processed an order which was not valid.

In the event that producer wishes to place an order for the reproduction of files which already contain a watermark, for example, according to the present invention, the recipient will require confirmation from the producer of the producer's derivation of right to place the order, before the order is executed. The derivation of right may take the form of a signed licence from the original producer, or a signed notarised note of the existence of an

appropriate licence. Indeed, the derivation of right may pass through multiple parties, in which case multiple authorisations will be required. Thus, the recipient may verify both that the order is authorised by the relevant rights holder, and that the order was placed by an authorised party.

In certain circumstances, a producer may wish to order reproduction of files which have already been released and are available to the recipient from another source. For example, the producer may wish to make available on the Internet a set of audio tracks which have already been released on compact disc. In that case, the producer need only specify to the recipient which files are to be reproduced, without having to transmit the files themselves. Thus, the signed order with the list of ISRC's may give sufficient information for the order to be executed, if the recipient has access to a database of files indexed by ISRC. Instead of ISRC's the producer may use a standard code to indicate the product on which the files were previously released, such as those used by the disc recognition service (DRS) operated by CDDB, an internet-based CD database.

Although the use of public/private key pairs is described above for the creation of digital signatures, the use of symmetric keys is also possible. However, this would require a separate key to be set up for each possible producer/recipient combination. Hence, the use of asymmetric keys is preferred unless the number of possible combinations is small.

CLAIMS

1. A method of selectively transferring a digital data file onto a medium for enabling mass reproduction of the digital data file, comprising:

obtaining said data file;

receiving authorisation data including encrypted data derived from a file identity code substantially uniquely identifying said data file;

deriving said file identity code from said data file;

comparing said file identity code with said encrypted data and inhibiting transferral of the data file onto the medium if the encrypted data does not correspond to said file identity code.

2. A method as claimed in claim 1, wherein said encrypted data is a digital signature of the authorisation data, the comparing step including decrypting the digital signature using a key corresponding to that used to encrypt the signature.

3. A method as claimed in claim 2, wherein the encrypted data is encrypted using a private key, and is decrypted using a corresponding public key.

4. A method as claimed in claim 2 or claim 3, wherein reproduction of the data file is inhibited if the key required for decryption of the signature does not correspond to an entry in a database.

5. A method as claimed in any preceding claim, wherein the authorisation data includes a specified time criterion, wherein reproduction of the data file is inhibited if current time information does not match the specified time criterion.

6. A method as claimed in any preceding claim, wherein the authorisation data includes a specified location criterion, wherein reproduction of the data file is inhibited if local location information does not match the specified location criterion.

7. A method as claimed in any preceding claim, wherein the authorisation data includes a specified identity code, wherein reproduction of the data file is inhibited if a predetermined identity code does not match the specified identity code.

8. A method as claimed in any one of claims 4 to 7, further comprising the step of generating an error message on inhibiting the reproduction of the data file.

9. A method as claimed in claim 8, further comprising the step of resuming the reproduction of the data file response to a user input command.

10. A method according to claim 8 or claim 9 further comprising the step of making a record of any reproduction of the data file after the generation of the error message.

11. A method as claimed in any preceding claim, wherein the file identity code is embedded in said data file.

12. A method as claimed in any one of claims 1 to 7, wherein the file identity code is derived from intrinsic characteristics of the data file.

13. A method as claimed in any preceding claim, wherein the medium is a master for creating multiple copies of the data file by a mechanical process.

14. A method as claimed in any one of claims 1 to 12, wherein the medium is a publicly accessible network.

15. A method of creating a reproduction command for enabling mass reproduction of a digital data file, comprising:

generating a digital signature of a file identity code substantially uniquely identifying the data file by means of an encryption key.

16. A method as claimed in claim 15, further including

processing said data file to embed therein the file identity code.

17. A method as claimed in claim 15, further including

deriving said file identity code from intrinsic characteristics of the data file.

18. A method as claimed in any one of claims 15 to 17, wherein the reproduction command further includes a specified time criterion, the digital signature being generated from said specified time criterion.

19. A method as claimed in any one of claims 15 to 18, wherein the reproduction command further includes a specified location criterion, the digital signature being generated from said specified location criterion.

20. A method as claimed in any one of claims 15 to 19, wherein the reproduction command includes an identity code, the digital signature being generated from said identity code.

21. A method as claimed in any one of claims 15 to 20, further including transmitting said digital signature.

22. A method as claimed in any one of claims 15 to 21, further including transmitting said data file.

23. A method as claimed in any one of claims 15 to 20, further including recording said data file and said digital signature on one or more removable media.

24. A method as claimed in any preceding claim, wherein the data file includes one or more of audio data, image data and video data.

25. A method as claimed in any preceding claim, wherein the data file includes computer program code.

26. Apparatus arranged to carry out the method of any one of claims 1 to 14.

27. A mastering apparatus including apparatus as claimed in claim 26.

28. A network server including apparatus as claimed in claim 26 or claim 27.

29. A computer including apparatus as claimed in claim 26 or claim 27.

30. A computer program including code arranged to perform each of the method steps of a method as claimed in claims 1 to 14 when executed by a computer as claimed in claim 29.

31. Apparatus arranged to carry out the method of any one of claims 15 to 25.

32. A computer including apparatus as claimed in claim 31.

33. A computer program including code arranged to perform each of the method steps of a method as claimed in claims 1 to 24 when executed by a computer as claimed in claim 32.

34. A signal comprising a digital signature of a file identity code substantially uniquely identifying a data file.

35. A signal as claimed in claim 34, wherein the file identity code is embedded in said data file such that the reproduction quality of the data file is substantially unaffected.

36. A signal as claimed in claim 34, wherein the file identity code is derived from intrinsic characteristics of the data file.

37. A signal as claimed in any one of claims 34 to 36, further including specified time criterion data, the digital signature being generated from said specified time criterion data.

38. A signal as claimed in any one of claims 34 to 37, further including specified location criterion data, the digital signature being generated from said specified location criterion data.

39. A signal as claimed in any one of claims 34 to 38, including an identity code, the digital signature being generated from said identity code.

40. A signal as claimed in any one of claims 34 to 39, wherein the digital file comprises one or more of: audio data, image data and video data.

41. A recording medium carrying a signal as claimed in any one of claims 34 to 40.

42. A method of rights management for copyright material, comprising:

creating and sending an order to reproduce the copyright material onto a medium for mass reproduction from an issuing party to a receiving party, the order comprising:

one or more digital data files comprising said copyright material and a digital signature generated by the issuing party of at least one substantially unique identity code identifying said data file or files.

43. A method as claimed in claim 42, further including validating the order by the receiving party and reproducing the copyright material only if the order is valid.

44. A method as claimed in claim 42 or claim 43, wherein the data files are watermarked with the corresponding identity code.

45. A method as claimed in claim 42 or claim 43, wherein the receiving party derives a characteristic code from each of the data files so as to obtain the corresponding identity codes.

46. A method substantially as herein described with reference to Figure 1 of the accompanying drawings.

47. A method as claimed in claim 46, further substantially as herein described with reference to Figure 3 of the accompanying drawings.

48. A method substantially as herein described with reference to Figure 2 of the accompanying drawings.

49. A method as claimed in claim 48, further substantially as herein described with reference to Figure 4 of the accompanying drawings.

50. A method as claimed in claim 48, further substantially as herein described with reference to Figure 5 of the accompanying drawings.

51. Apparatus substantially as herein described with reference to Figure 1 of the accompanying drawings.

52. Apparatus as claimed in claim 51, further substantially as herein described with reference to Figure 3 of the accompanying drawings.

53. Apparatus substantially as herein described with reference to Figure 2 of the accompanying drawings.

54. Apparatus as claimed in claim 53, further substantially as herein described with reference to Figure 4 of the accompanying drawings.

55. Apparatus as claimed in claim 53, further substantially as herein described with reference to Figure 5 of the accompanying drawings.

Fig. 1

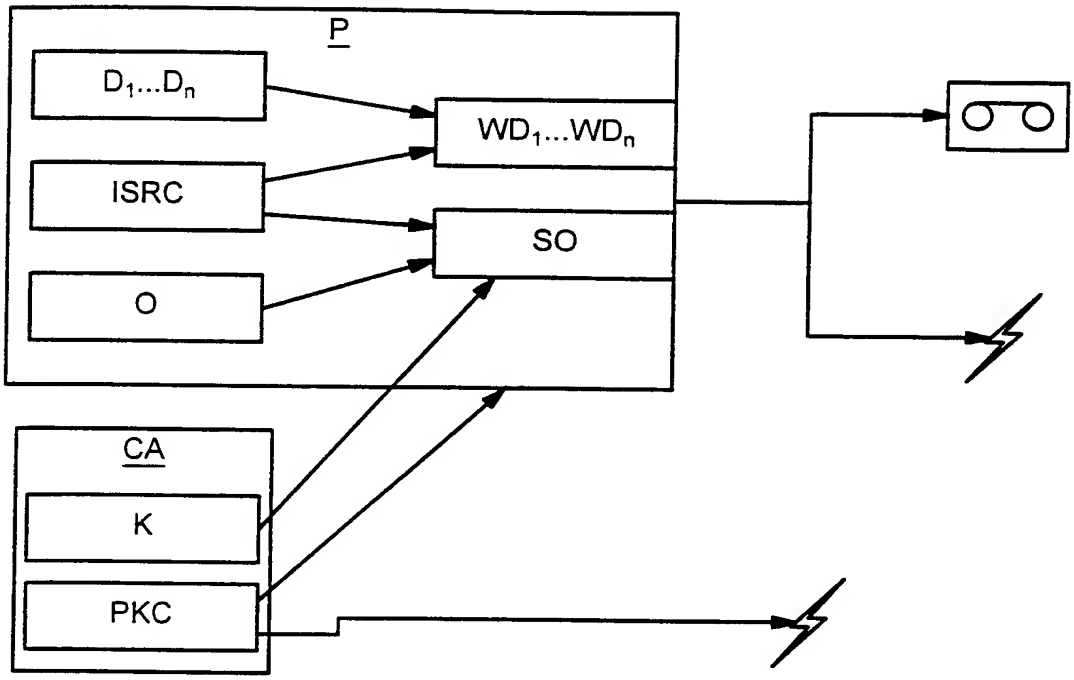

P
D1...Dn
WD1...WDn
ISRC
SO
O
CA
K
PKC

Fig. 2

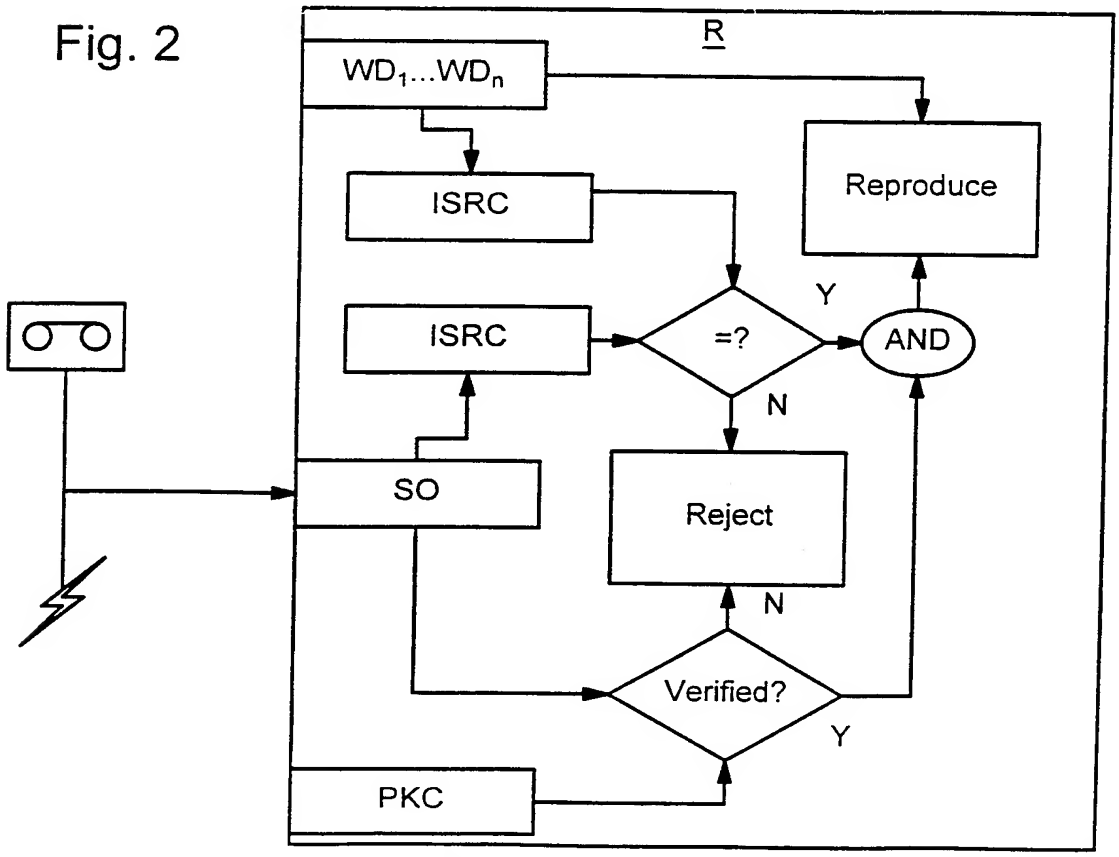

R
WD1...WDn
ISRC
Reproduce
ISRC
=?
Y
AND
N
SO
Reject
N
Verified?
Y
PKC

Fig. 3

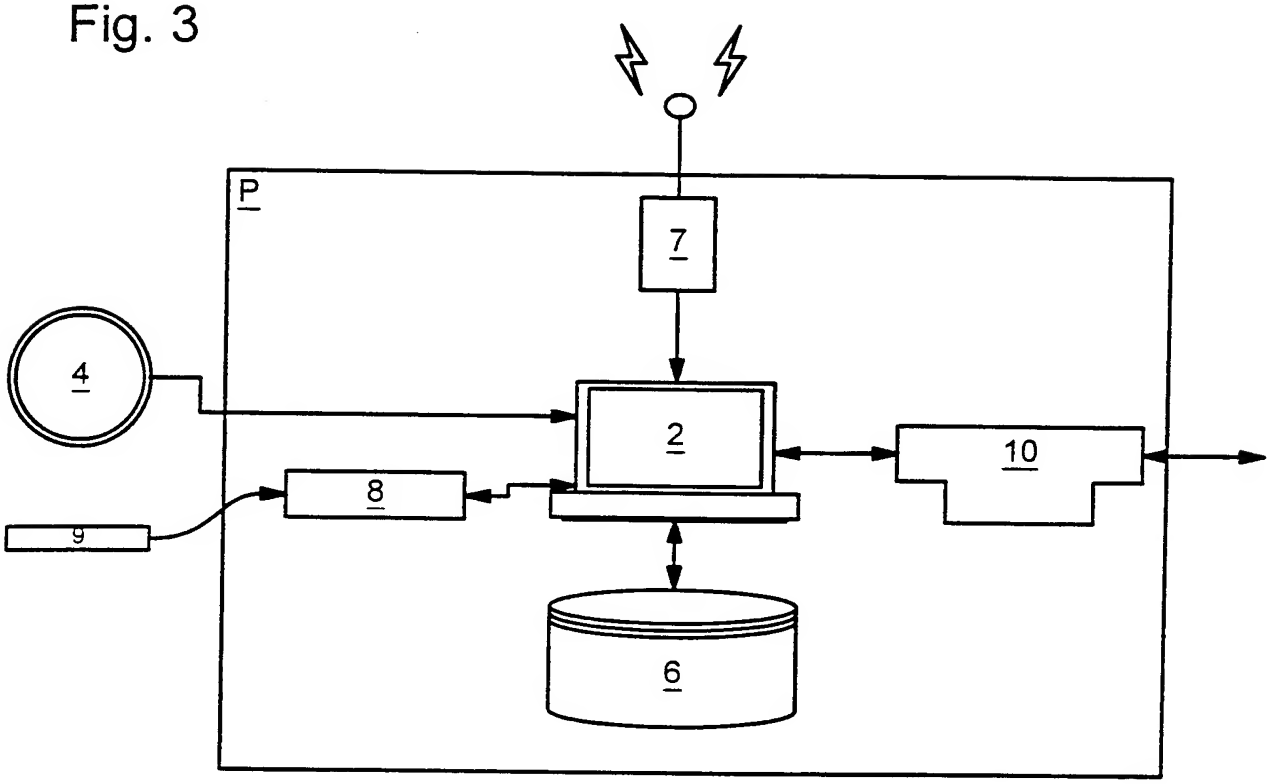


Fig. 4

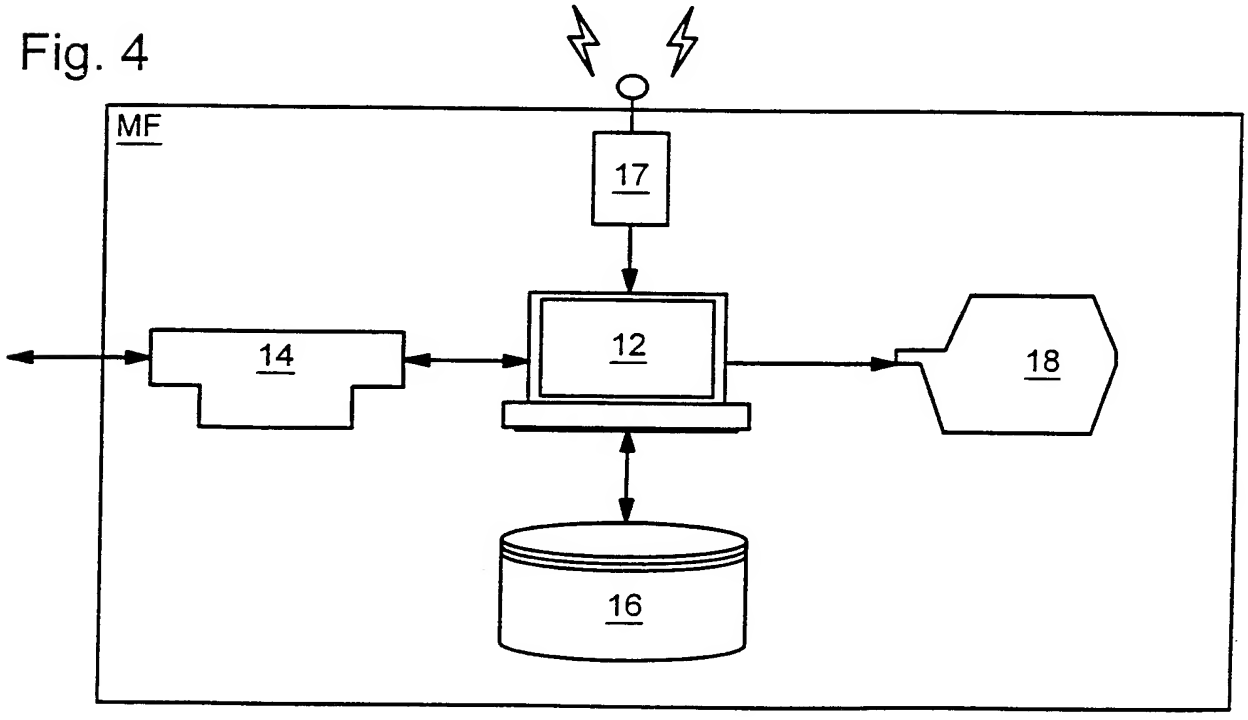
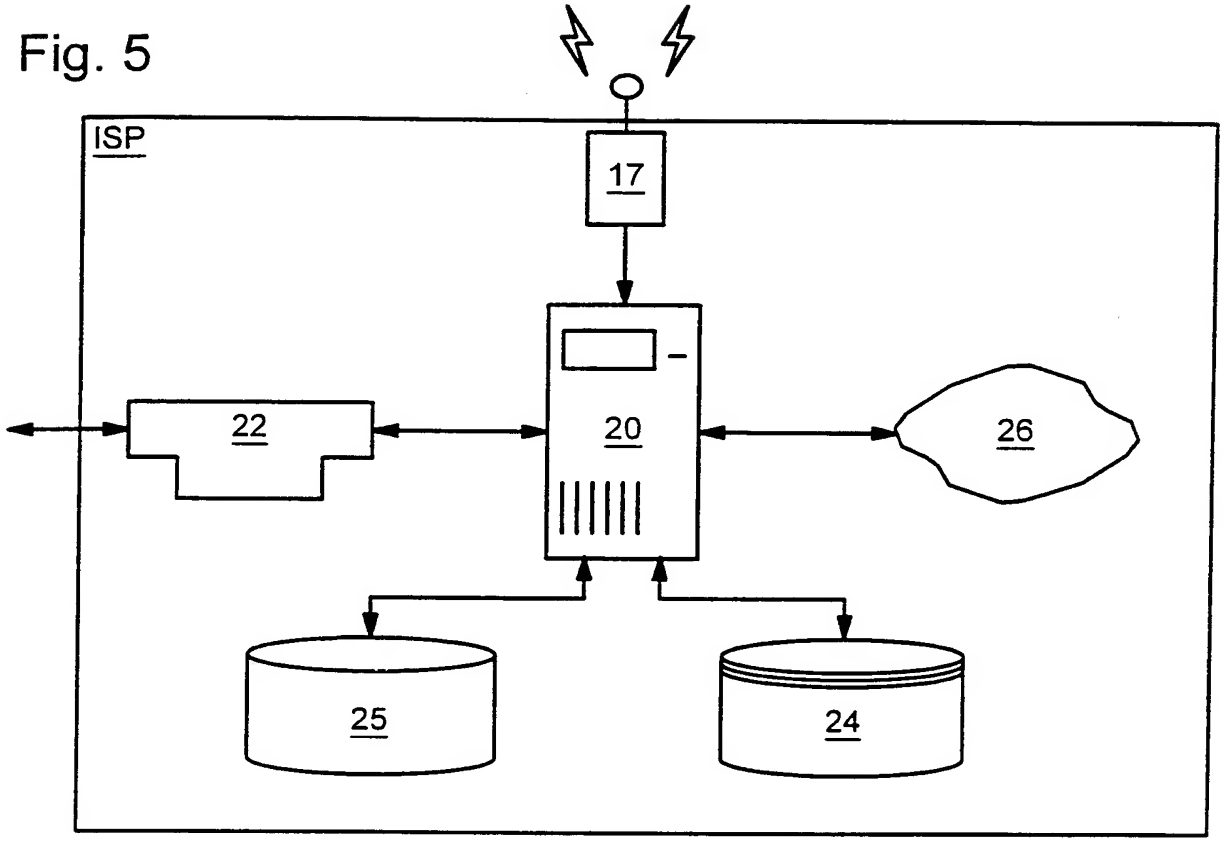


Fig. 5



INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 00/02985

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 845 733 A (SUN MICROSYSTEMS INC) 3 June 1998 (1998-06-03)	15-17, 19,23, 25, 31-35, 38,41
A	abstract column 1, line 37 -column 2, line 33 column 3, line 37 -column 4, line 28 column 5, line 29 - line 45 column 7, line 17 - line 44 figure 3	1-3,6,7, 11,26, 29,39,42

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 December 2000	09/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schiwy-Rausch, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat...onal Application No
PCT/GB 00/02985

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 849 658 A (NCR INT INC) 24 June 1998 (1998-06-24) abstract column 1, line 23 - line 50 column 2, line 40 -column 3, line 50	1-3,7,8, 15,16, 34,35, 42,43
A,P	US 6 021 491 A (RENAUD BENJAMIN J) 1 February 2000 (2000-02-01) column 3, line 22 -column 4, line 29 column 6, line 40 -column 7, line 57	1,2,7, 11,15, 16,20, 25,26, 29-35, 39,41,42
A	EP 0 762 758 A (SONY CORP) 12 March 1997 (1997-03-12) abstract column 2, line 17 - line 47 column 3, line 24 -column 4, line 45 column 9, line 23 -column 10, line 7 claim 1; figure 1	1,5-11, 13,15, 18-20, 24,26,31

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 00/02985

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0845733 A	03-06-1998	US 6021491 A	01-02-2000
		US 5958051 A	28-09-1999
		JP 10326078 A	08-12-1998
EP 0849658 A	24-06-1998	JP 10312335 A	24-11-1998
US 6021491 A	01-02-2000	EP 0845733 A	03-06-1998
		JP 10326078 A	08-12-1998
		US 5958051 A	28-09-1999
EP 0762758 A	12-03-1997	CN 1152170 A	18-06-1997
		JP 9128874 A	16-05-1997
		US 5703859 A	30-12-1997
		US 6115533 A	05-09-2000

they do not match. The use of an intended recipient code in the order may prevent the pirate from replaying or redirecting an order to another recipient acting in concert with the pirate, such that the other recipient may claim that the order was apparently legitimate.

If the order data O includes a code identifying specific equipment on which the order is to be carried out, the recipient R checks the identity of the equipment under its control and routes the order to the specified equipment. If the specified equipment is not available, the order is rejected.

If the order data O includes a specification of the geographical area within which the order is to be carried out, the recipient R checks the specified area and rejects the order if the known geographical location of the recipient R does not fall within the specified area. The known geographical location may be prestored by the recipient's reproduction equipment, or may be read from a GPS receiver. The use of a specified location or specified equipment helps to prevent recipients from processing authorised orders at one site or one set of equipment, which is open to inspection, and producing unauthorised copies at a different site or on different equipment using duplicate order data O.

To prevent inadvertent or deliberate duplication of orders, the recipient R may store a database of previous orders and reject any subsequent orders for which the order data is identical (or substantially so) to that of a previous order. Orders for which the validity duration has expired may be deleted from the database, since duplicate orders would then be rejected on the basis of the validity duration.

Although equipment which lacks order data checking could be used to reproduce unauthorised copies, piracy investigation can be concentrated on operators of such equipment. Moreover, the recipient may be required to use order data checking, either by law or to comply with a quality standard, such as ISO 9000.

The recipient R may automatically send an acknowledgement message back to the producer P, including for example an identification of the order